FedRAMP Initial Review Results

<Agency, CSP Name>

<Information System Name>

<Agency, CSP FIRR v #.##>

<Date>

Template Version 1.0

FEDRAMP INITIAL REVIEW RESULTS

EXECUTIVE SUMMARY

<**Corporation Name**> submitted its Security Plan with Attachments <**plus its Security Assessment material**> for FedRAMP Initial Review of their cloud-based <**Information System Name (Abbreviation**); see Table 1>. The <**Info System Abbreviation**> system security package, including all attachments, was reviewed for compliance with FedRAMP requirements for system security safeguards.

Table 1. <Abbreviation> Summary

<Corporation> Cloud-based System <Abbreviation>	
FIPS 199 Categorization	<Low, Moderate>
Cloud Service Model	<Infrastructure, Platform, Software> as a Service <(IaaS), (PaaS) (SaaS)>
Deployment Model	<Public, Private, Community, Hybrid>
FedRAMP Path	<Agency, Cloud Service Provider (CSP)-supplied, Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO)>

This report summarizes the results of the FedRAMP Initial Review performed by FedRAMP staff. All metrics and comments provided in this document are based on checklists standardized for consistency and applicability.

Based on these results, it is recommended that <**Information System Abbreviation**> documentation be [**considered < >, returned to the Cloud Service Provider (CSP) for rework**].

1. ASSESSMENT PROCESS

The Federal Risk Authorization Management Program (FedRAMP) review process is divided into two phases: (1) the FedRAMP Initial Review (FIR) and (2) the FedRAMP Detailed Review. During the FIR, FedRAMP Program Management Office (PMO) examines the overall completeness and quality of the submitted documents (Authorization Package), and spot checks key security controls.

The results of evaluating the package are documented using a checklist with various Yes or No questions. These criteria are rolled into one, overall percentage to indicate the number of compliant ("Yes") checkmarks. A second breakout, showing just Showstoppers and Critical Controls, provides a more specific compliance metric.

Table 2 below summarizes the results of the FIR using the checklist criteria. The percentages indicate the number of compliant checkmarks, which could be "Yes" or "No," depending on the checklist.

If a document(s) successfully completes the FIR, it continues to the next step, as determined by its path. <**For the Joint Authorization Board (JAB) Provisional-Authorization to Operate (ATO) (P-ATO) path, the Authorization Package will be assigned a FedRAMP Information System Security Officer (ISSO) to perform the Detailed Review.** > <**For an Authorization**

Package on the Agency ATO or Cloud Service Provider (CSP) Supplied path, the document is submitted to the FedRAMP Director for review. > <**At this point, Agency ATO and JAB P-ATO Path packages will be designated as FedRAMP In-Process and CSP-supplied will be designated as FedRAMP Ready.**> This process is more thoroughly discussed in the *FedRAMP Review and Approve Process Standard Operating Procedure (SOP)*, available at www.FedRAMP.gov.

2. ASSESSMENT RESULTS AND KEY FINDINGS

The attached FedRAMP Initial Review Checklists document more comprehensive information regarding the results of the FIR. One or two Key Findings from each checklist is referenced in Table 2 below as a sample.

To complete Table 2, below, review the accompanying checklists. Each header (alphabetized for ease of reference) represents one of the checklist categories.

For each document reviewed, provide one or two key findings as examples.

Take the total number of "Yes" checkmarks, divide by the total number of line items in the checklist and insert the resulting percentage in Table 2 below.

Please delete this instruction box prior to sending the results.

Table 2. FedRAMP Initial Review Results

Checklist	Percent Compliant	# Pass/ # Total	Key Findings
SSP			
Readability			
SAP			
SAR			
POA&M			

The **< Info System Abbreviation**> System Security Plan (SSP) showed significant effort which, <**status e.g., however, was not adequate to meet the criteria**>. The questions asked in the checklists <**describe, e.g., identified several areas of weakness in the Security Plan and its attachments. Of the total of 114 questions, 56 were FedRAMP compliant (49%). Of the 13 Showstoppers and 17 Critical Controls (30, total), 7 were FedRAMP compliant (23%).**> The checklists attached provide details.

The attached **< Info System Abbreviation**> SSP Initial Review Checklists document more comprehensive information regarding the results of the FIR of the **< Info System Abbreviation**> SSP. All required attachments were available, although the Rules of Behavior and Configuration Management Plan were embedded in other documents. Showstoppers <**did, did not**> stop this Initial Review.

3. CONCLUSION/RECOMMENDATIONS

Based on the above assessment results and key findings, the recommendation is that <**Information System Abbreviation**> <**is, is not**> suitable for posting to *FedRAMP.gov*.

STATUS SUMMARY:

☐ Passed Initial Review (see Next Step, below)

☐ Designate as FedRAMP Ready – Pending Approval by FedRAMP Director, or his Proxy (CSP-supplied)

☐ Designate as FedRAMP In Process – FedRAMP Director (or his Proxy) Approval (Agency ATO or JAB P-ATO)

☐ Return to Provider for Additional Information

☐ Return to Provider for Rework *If "Return to Provider for Rework" is selected, delete the following box.*

☐ Due to Severity of Findings, Provider is Not to Resubmit to FedRAMP for at Least <###> <**Days, Months**>; Identified Findings Must be Addressed Throughout the Document(s) as Applicable

NEXT STEP IF PASSED INITIAL REVIEW:

☐ Return Package to OMB MAX for Another Review

☐ JAB P-ATO Path – Assign ISSO; Perform Detailed Review; FedRAMP In Process

☐ CSP-Supplied Path – Schedule Briefing with 3PAO and CSP to Review Package with FedRAMP Director

☐ Agency ATO Path – To FedRAMP Director, or his Proxy, for Approval

4. ACRONYMS AND ABBREVIATIONS

Table 3. Acronyms and Abbreviations

Acronym	Definition
3PAO	Third Party Assessment Organization
AC	Access Control (NIST Security Control Family)
AO	Authorizing Official
AT	Awareness and Training (NIST Security Control Family)
ATO	Authorization to Operate
AU	Audit and Accountability
CA	Security Assessment and Authorization (NIST Security Control Family)
CIS	Control Implementation Summary
CM	Configuration Management (and NIST Security Control Family)
Config	Configuration
ConMon	Continuous Monitoring
CP	Contingency Plan
CP	Contingency Planning (NIST Security Control Family)
CSP	Cloud Service Provider
CTW	Control Tailoring Workbook
DHS	Department of Homeland Security
DOD	Department of Defense
FedRAMP	Federal Risk Authorization Management Program
FIPS	Federal Information Processing Standards
FIR	FedRAMP Initial Review
FIRR	FedRAMP Initial Review Results
FISMA	Federal Information Security Management Act of 2002
GSA	General Services Administration
HIDS	Host-based Intrusion Detection System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Security
IA	Identification and Authentication (NIST Security Control Family)
IaaS	Information as a Service
Info	Information
IR	Incident Response
ISSO	Information System Security Officer
JAB	Joint Authorization Board
MA	Maintenance (NIST Security Control Family)
Mgmt	Management
MP	Media Protection (NIST Security Control Family)
N/A	Not Applicable
NIST	National Institute of Standards and Technology
P-ATO	Provisional-ATO
PaaS	Platform as a Service
PE	Physical and Environment Protection (NIST Security Control Family)
PIA	Privacy Impact Assessment
PL	Planning (NIST Security Control Family)
PMO	Program Management Office
POA&M	Plan of Action and Milestones
PS	Personnel Security (NIST Security Control Family)
PTA	Privacy Threshold Analysis
Pub	Publication
RA	Risk Assessment (and NIST Security Control Family)

Acronym	Definition
Rev	Revision
RoB	Rules of Behavior
SA	Security Assessment
SA	System and Services Acquisition (NIST Security Control Family)
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAP	Security Assessment Plan
SAR	Security Assessment Report
SC	System and Communications Protection (NIST Security Control Family)
Sec	Security
SI	System and Information Integrity (NIST Security Control Family)
SP	Special Publication
SSP	Security Plan
TR	Technical Representative

5. GLOSSARY

The following definitions apply to the specified terms.

Table 4. Glossary

Term	Definition
Completeness	Presence of expected document, artifact, or information
Critical	Review of a designated controls for completeness and quality
Defect	Any problem within a reviewed document not specifically called out (not identified as: Completeness, Critical, Showstopper, Quality, Verification)
Detailed Review	In-depth security review of an Authorization Package presented to FedRAMP; ISSO named and associated with the Authorization Package; review by named ISSO, who performs an in-depth review of security control implementation statements and applicability of evidence prior to submission to JAB TRs
FedRAMP Compliant	Adheres to federal security standards and regulations applied to use of the cloud
FedRAMP Path	A security Authorization Package reviewed in accordance with FedRAMP criteria according to provider presentation as Agency ATO, CSP supplied, or JAB P-ATO.
FedRAMP Ready	Systems which have had their Authorization Package reviewed by the FedRAMP PMO and at a minimum, completed the PMO Initial Review process
Four Cs	Clear, Concise, Consistent, and Complete
Initial Review	First reading of an Authorization Package presented to FedRAMP; among the first steps is assessing the Four Cs, determining readability, and ensuring implementation statements are present, complete, and in line with the associated control; applies to all paths
Key Element	A selection of NIST SP 800-53, Rev 4, Cloud, and FedRAMP requirements and guidance considered critical to system security
Quality	A general check for document problems with Clarity, Consistency, and Conciseness
Readability	Determination of reading ease defined by application of Severity levels (Low, Medium, High) against the Four Cs
Showstopper	Missing, incomplete, or weak critical security controls that must be addressed before documents continue through FedRAMP review process

Term	Definition
Spot Check	An inspection or investigation performed on a random, limited number of instances; an arbitrary selection of security package components reviewed closely to ensure provider is consistent with appropriate depth of responses
Verification	Initial assurance of consistency and correctness of documents, artifacts, and/or information